WHAT IS CLAIMED IS:

1. A system for securely embedding a watermark representing message data into movie data consisting of one or more frames of a digital image sequence, and displaying one or more frames of the digital image sequence containing the embedded watermark, comprising:

means for providing a secure environment;

means for combining the movie data with the watermark within the secure environment to produce watermarked movie data; and

means for forming a displayed image from the watermarked movie data within the secure environment.

2. The system according to Claim 1, wherein the movie data is uncompressed data.

3. The system according to Claim 1, wherein the movie data is compressed data.

4. The system according to Claim 1, further including means for storing the movie data within the secure environment.

5. The system according to Claim 1, wherein the movie data has been encrypted to produce encrypted data representing the digital image sequence, and further including means for decrypting the encrypted data within the secure environment to produce movie data.

6. The system according to Claim 1, wherein the movie data has been compressed and encrypted to produce compressed and encrypted data representing the digital image sequence, and further including means for decrypting the compressed and encrypted data within the secure environment to

produce compressed data, and means for decompressing the compressed data within a secure environment to produce movie data.

7. The system according to Claim 6, further including means for storing the compressed and encrypted data.

8. The system according to Claim 6, further including means for storing the compressed data within the secure environment.

9. The system according to Claim 1, wherein the secure environment is provided by a combination of physical and logical protection techniques.

10. A system for securely embedding watermark information in one or more frames of a digital image sequence, comprising:

a) means for providing a secure environment;

b) means for generating a watermark key for one or more frames in the digital image sequence within the secure environment;

c) means for generating a watermark message for one or more frames in the digital image sequence within the secure environment;

d) means for generating a watermark pattern for one or more frames using the corresponding watermark key and watermark message within the secure environment; and

e) means for combining the watermark pattern with the corresponding frame of the digital image sequence within the secure environment.

11. The system according to Claim 10, wherein means for generating a watermark key includes means for updating the key throughout the digital image sequence.

12. The system according to Claim 10, wherein means for generating a watermark message includes means for generating a validated time stamp.

13. The system according to Claim 10, further including means for securely sending the watermark key to a remote database.

14. The system according to Claim 10, further including means for securely sending the watermark message to a remote database.

15. The system according to Claim 10, further including means for acquiring a secure watermark root key from a remote server and using the watermark root key in generating the watermark key.

16. The system according to Claim 15, wherein the watermark root key is an initialization key.

17. The system according to Claim 10, further including means for acquiring a secure watermark root message from a remote server and using the watermark root message in generating the watermark message.

18. The system according to Claim 17, wherein the watermark root message includes a unique theater ID.

19. The system according to Claim 17, wherein the watermark root message includes a unique presentation ID.

20. The system according to Claim 10, wherein the secure environment is provided by a combination of physical and logical protection techniques.

21. A method for securely embedding a watermark representing message data into movie data consisting of one or more frames of a digital image sequence, and displaying one or more frames of the digital image sequence containing the embedded watermark, comprising the steps of:

providing a secure environment;

combining the movie data with the watermark within the secure environment to produce watermarked movie data; and

forming a displayed image from the watermarked movie data within the secure environment.

22. The method according to Claim 21, wherein the movie data is uncompressed data.

23. The method according to Claim 21, wherein the movie data is compressed data.

24. The method according to Claim 21, further including the step of storing the movie data within the secure environment.

25. The method according to Claim 21, wherein the movie data has been encrypted to produce encrypted data representing the digital image sequence, and further including the step of decrypting the encrypted data within the secure environment to produce movie data.

26. The method according to Claim 21, wherein the movie data has been compressed and encrypted to produce compressed and encrypted data representing the digital image sequence, and further including the steps of decrypting the compressed and encrypted data within the secure environment to

produce compressed data, and decompressing the compressed data within a secure environment to produce movie data.

27. The method according to Claim 26, further including the step of storing the compressed and encrypted data.

28. The method according to Claim 26, further including the step of storing the compressed data within the secure environment.

29. The method according to Claim 21, wherein the secure environment is provided by a combination of physical and logical protection techniques.

30. A method for securely embedding watermark information in one or more frames of a digital image sequence, comprising the steps of:

a) providing a secure environment;

b) generating a watermark key for one or more frames in the digital image sequence within the secure environment;

c) generating a watermark message for one or more frames in the digital image sequence within the secure environment;

d) generating a watermark pattern for one or more frames using the corresponding watermark key and watermark message within the secure environment; and

e) combining the watermark pattern with the corresponding frame of the digital image sequence within the secure environment.

31. The method according to Claim 30, wherein the step of generating a watermark key includes the step of updating the key throughout the digital image sequence.

32. The method according to Claim 30, wherein the step of generating a watermark message includes the step of generating a validated time stamp.

33. The method according to Claim 30, further including the step of securely sending the watermark key to a remote database.

34. The method according to Claim 30, further including the step of securely sending the watermark message to a remote database.

35. The method according to Claim 30, further including the steps of acquiring a secure watermark root key from a remote server and using the watermark root key in generating the watermark key.

36. The method according to Claim 35, wherein the watermark root key is an initialization key.

37. The method according to Claim 30, further including the steps of acquiring a secure watermark root message from a remote server and using the watermark root message in generating the watermark message.

38. The method according to Claim 37, wherein the watermark root message includes a unique theater ID.

39. The method according to Claim 37, wherein the watermark root message includes a unique presentation ID.

40. The method according to Claim 30, wherein the secure environment is provided by a combination of physical and logical protection techniques.